ABSTRACT

A PUBLIC KEY ENCRYPTION SYSTEM

This invention relates to a variant of the El-Gamal public key encryption scheme, which is provably secure against an adaptively chosen ciphertext adversary using standard public-key cryptography assumptions i.e. not the random oracle model. This new scheme has roughly half the computational overhead and similar communication overhead as the scheme by Cramer-Shoup.

[Figure 1]